Access Control

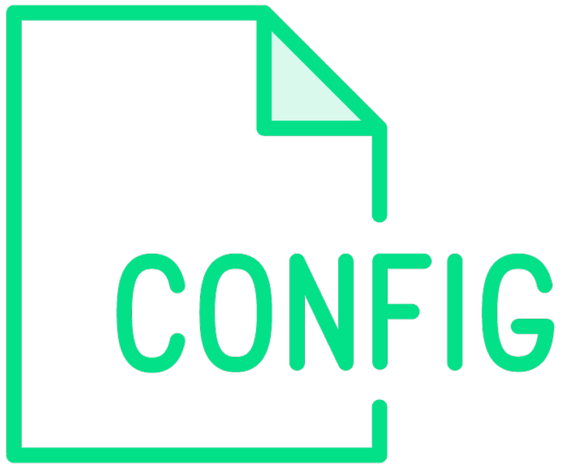
Paul Mooney
Chief Software Architect, Microsoft MVP

@daishisystems | www.insidethecpu.com

Overview

Access Control

- Trusted system objects for authorization
- Session Management with JWT
- Secure and reliable access authorization



Standard Configuration

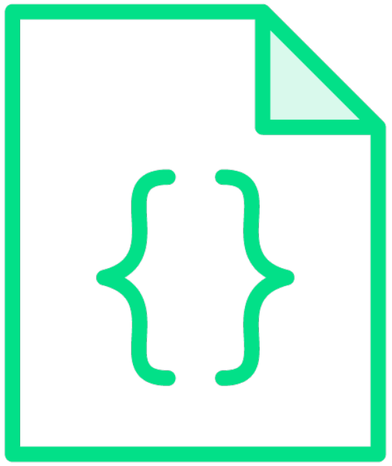
- Store and utilize session token
- Use singular component for authorization
- Secure access control failure with "defer"
- Deny access if configuration inaccessible
- Enforce authorization controls on every request
- Separate privileged logic from application code

Files and Other Resources

- Protect files and safeguard critical assets
- Strong authentication mechanisms for user verification
- Authorization mechanisms for determining access levels
- Role-based and attribute-based access control
- Fine-grained permissions and access restrictions
- Auditing and logging for accountability

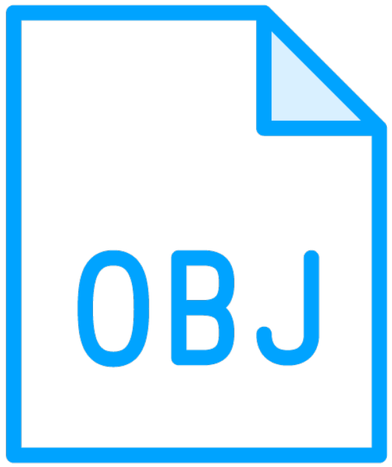
Protected URLs

- Protected URLs ensure web application security
- Proper authentication for verifying user identity
- Authorization based on roles and permissions
- Configure access controls on server-side and client-side
- Regularly review and update access control settings
- Implement additional security measures for protection



Protected Functions

- Protect functions to prevent unauthorized access
- Authentication and authorization for controlled access
- Strong authentication mechanisms ensure authorized users
- Fine-grained access controls for protected functions
- Regularly review and update access control settings
- Implement logging and auditing mechanisms for accountability

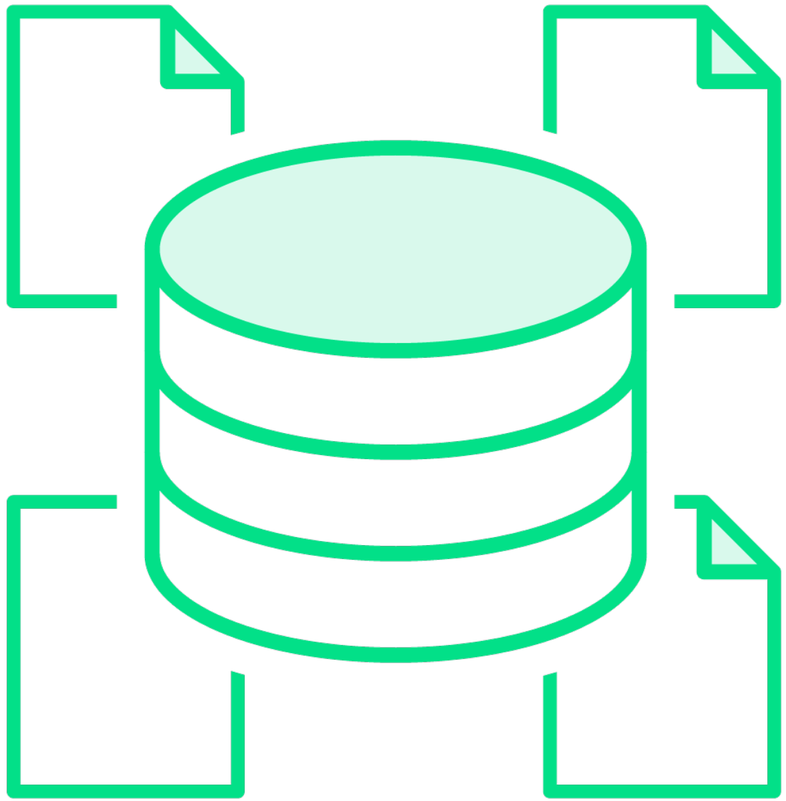


Direct Object References

- Direct object references risk unauthorized access
- Implement robust access controls
- Authentication and authorization mechanisms required
- Authentication verifies user and authorization grants permissions
- Use various authentication and authorization techniques
- Regularly review and update access control settings

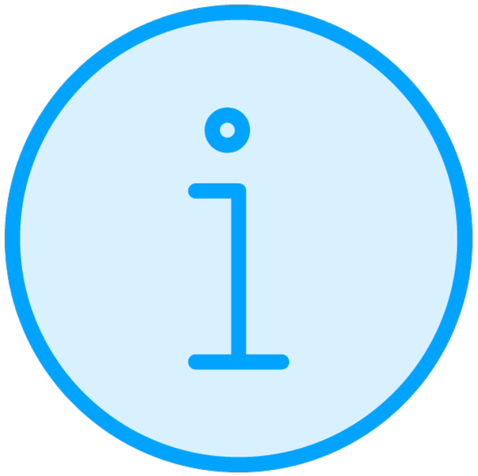
Services

- Services require proper access controls
- Authentication and authorization mechanisms required
- Use various authentication and authorization techniques
- Configure access controls for each service
- Regularly review and update access control settings
- Implement secure communication and monitoring



Application Data

- Protect application data with access controls
- Implement robust authentication and authorization mechanisms
- Use various authentication and authorization techniques
- Configure access controls for each data entity
- Regularly review and update access control settings
- Employ encryption, secure storage, and backups



User Attributes and Policy Information

- User and data attributes influence access control
- Implement authentication and authorization mechanisms
- Consider user attributes for access decisions
- Consider data attributes for access decisions
- Use attribute-based access control (ABAC)
- Regularly review and update access control policies

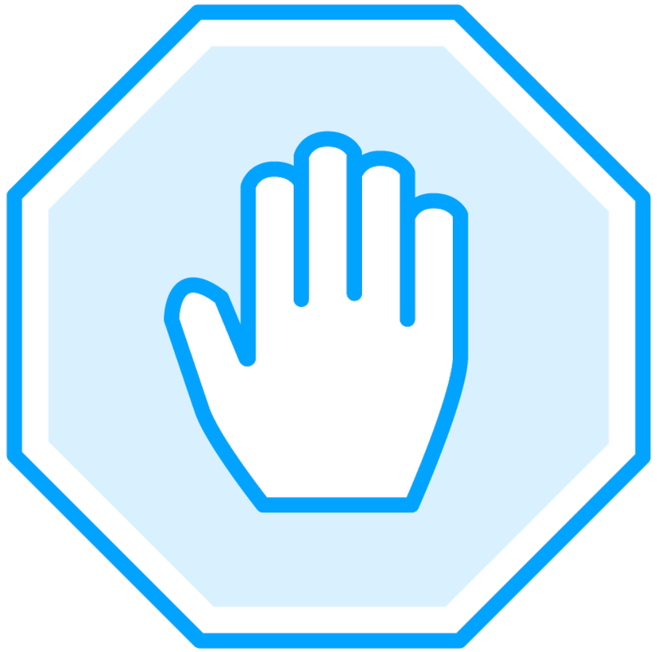
Best Practices

- Align server-side and presentation layer
- Encrypt and maintain data integrity
- Follow defined business rules
- Set transaction limits to prevent DoS
- "Referer" header is not sufficient
- Re-evaluate authorization for long sessions
- Implement user account auditing
- Disable accounts and terminate sessions
- Assign minimum privilege for external accounts

Summary

Access Control

- Importance of access controls
- Trusted system objects for authorization
- Secure access with JSON Web Tokens
- File and resource protection
- Protected URLs and functions
- Direct object references and granular access
- Access controls for application services
- Protection of application data
- Best practices for access controls

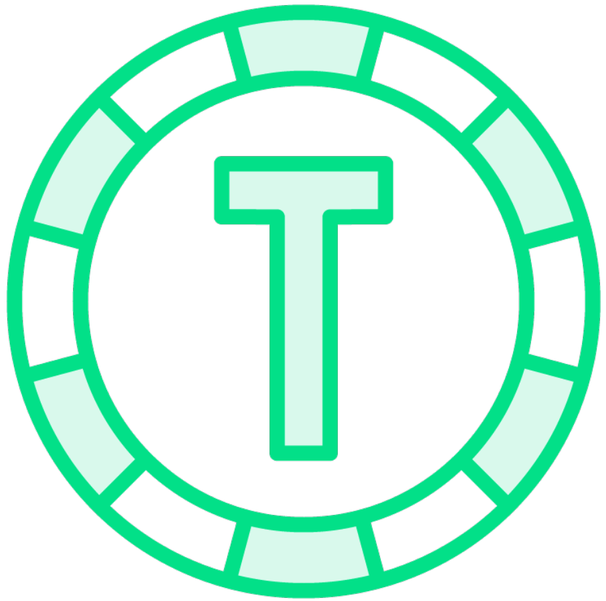


Access Controls

- Restrict session data
- Only accessible to authenticated user
- User isolation
- Access restriction
- Maintain session privacy
- Prevent data leakage

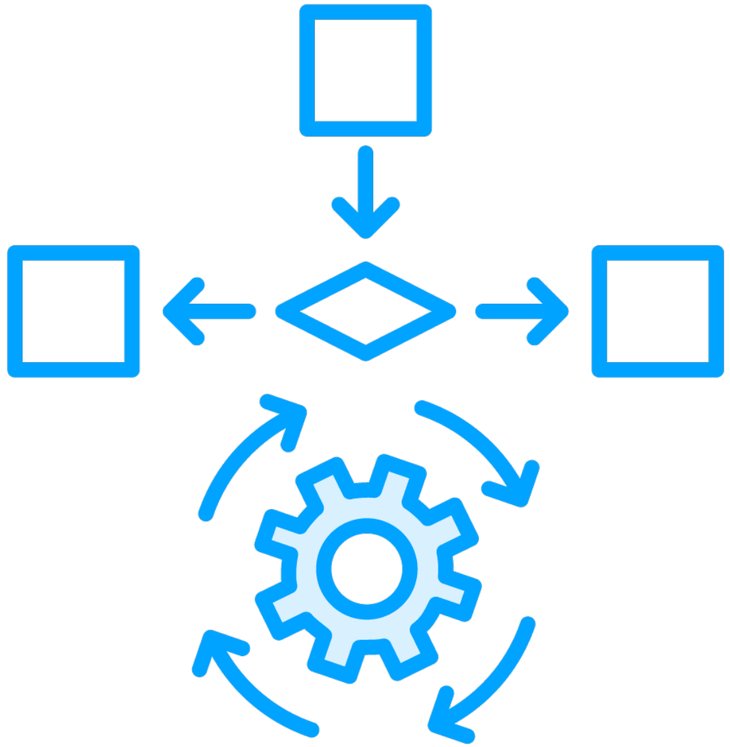
Man-in-the-middle (MITM) Attacks

- Intercept and hijack user sessions
- Use HTTPS
- Secure channel for communication



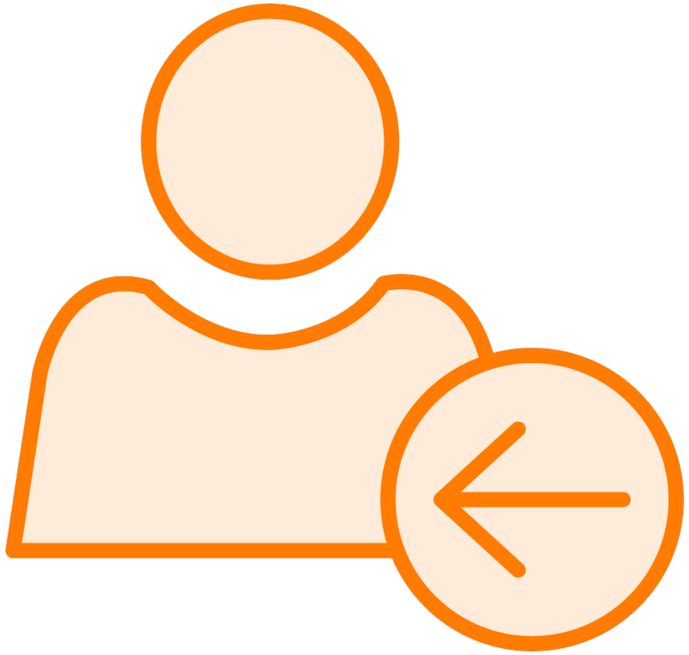
Tokens and Logout

- Per-request tokens
- Logout functionality



Critical Operations

- Per-request basis
- Each operation has a unique token
- Limited validity



Logout Functionality

- Session termination
- Disconnect from authenticated pages
- Connection termination

Demo

Secure Session Management

Communicating Authentication Data

Single-factor authentication

- Single factor for identification
- Easy to implement
- Least secure

Multi-factor authentication

- Multiple factors of identification
- More secure than single-factor
- More complex to implement

Biometric authentication

- Physical or behavioral characteristic
- Most secure type of authentication
- Expensive and difficult to implement

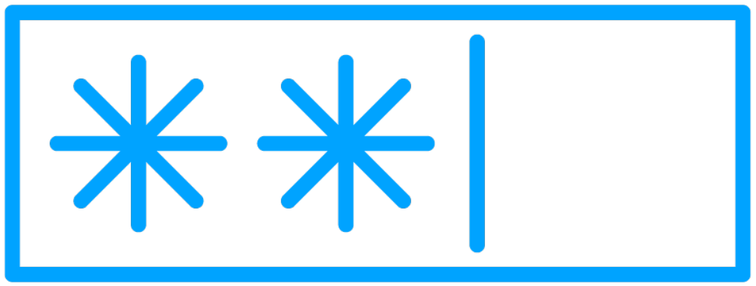
Common Authentication Protocols

- OAuth and OpenID Connect
- Limited access to resources
- 3rd party authentication
- Complex implementation
- Standardized way to authenticate users
- Use secure transport protocols
- Validate all input data
- Principle of least privilege
- Stay up to date

Secure Communication Protocols

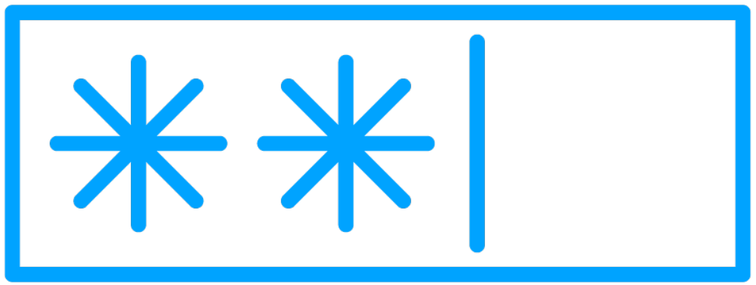
- Transport Layer Security (TLS)
- Secure Sockets Layer (SSL)
- Properly configuring certificates
- Disable outdated cryptographic ciphers
- Apply the latest security patches
- Use HTTP POST

Validating & Storing Authentication Data



Password Security Best Practices

- Hashing
- Salting
- Encryption



Password Policies

- Password length
- Password complexity
- Expiration date

Password Storage Options

Hashing

Fixed length

Encrypted

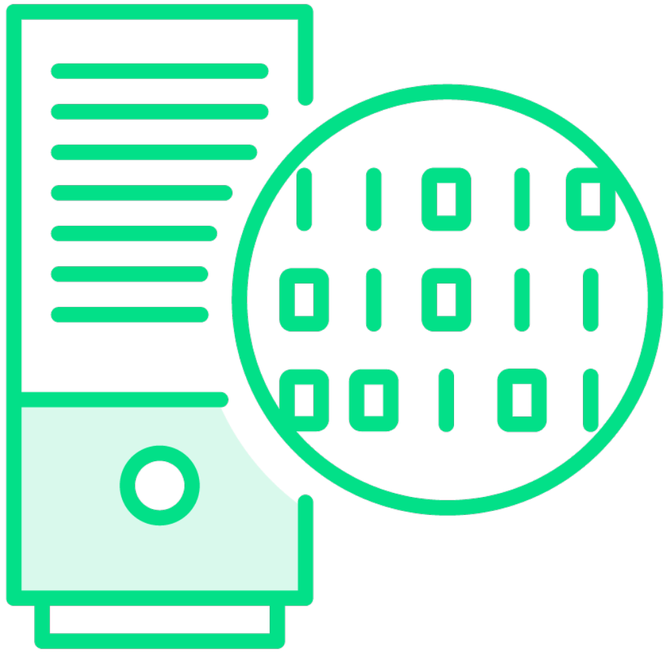
One-way

Salting

Random characters

Precomputed hash tables

Unique per password

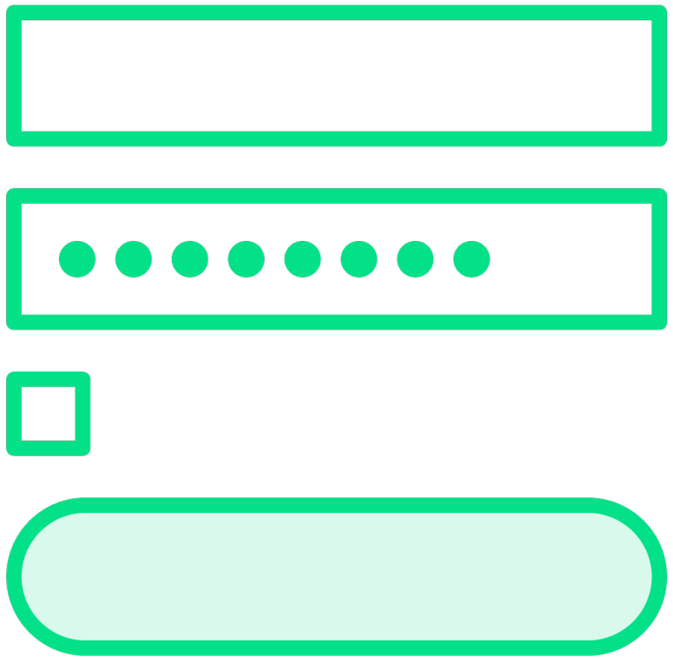


Supported Hashing Algorithms

- Bcrypt
- Scrypt
- Salt value per password

Demo

Single-factor Authentication



Password Policies

- Password complexity
- Hashing
- Salting
- Expiration
- Account lockout
- Policies versus convenience

Password Reset

- Requesting a reset
- Token storage
- Reset link generation
- Reset password page
- Password update
- Token expiration
- Token revocation
- Logging
- Error handling

Demo

Multi-factor Authentication

Summary

Authentication & Password Management

- Secure implementation guidelines
- Authentication types
- Common protocols
- Secure communication protocols
- Password security best practices
- SFA and MFA demos